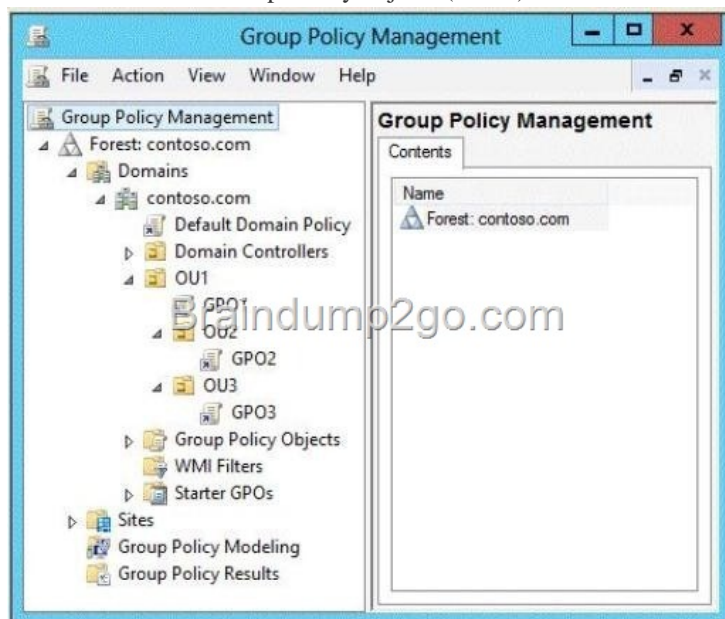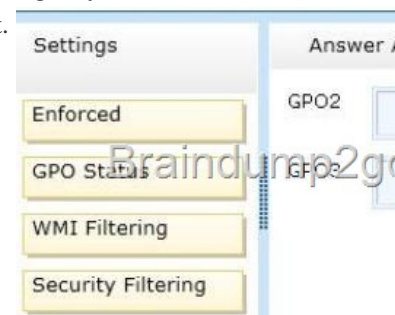# Official 2014 Latest Microsoft 70-411 Exam Dump Free Download(191-200)!
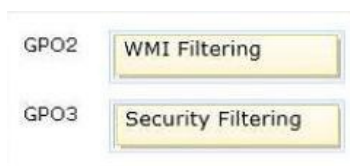
QUESTION 191 Drag and Drop Question Your network contains an Active Directory domain named contoso.com. All client computers run Windows 8. Group Policy objects (GPOs) are linked to the domain as shown in the exhibit. (Click the Exhibit button.)

GPO2 contains computer configurations only and GP03 contains user configurations only. You need to configure the GPOs to meet the following requirements: - Ensure that GPO2 only applies to the computer accounts in OU2 that have more than one processor. - Ensure that GP03 only applies to the user accounts in OU3 that are members of a security group named SecureUsers. Which setting should you configure in each GPO? To answer, drag the appropriate setting to the correct GPO. Each setting may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
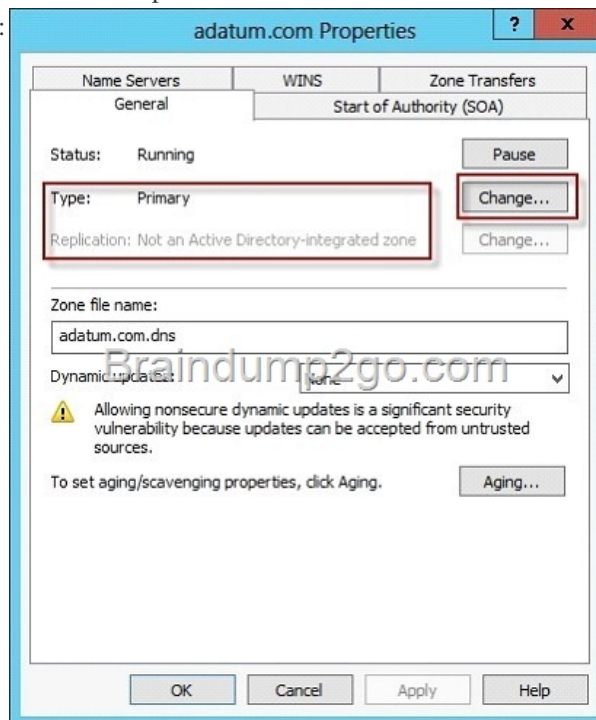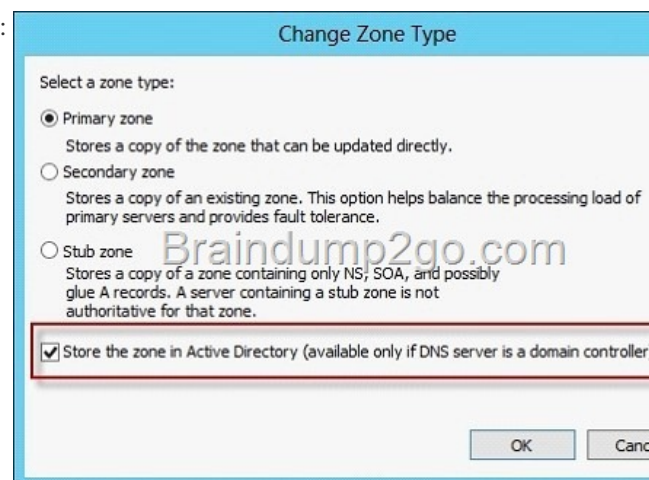

Answer:

] QUESTION 192 Your network contains an Active Directory domain named contoso.com.You have a standard primary zone names contoso.com. You need to ensure that only users who are members of a group named Group1 can create DNS records in the contoso.com zone. All other users must be prevented from creating, modifying, or deleting DNS records in the zone. What should you do first? A.   Run the Zone Signing Wizard for the zone. B.   From the properties of the zone, change the zone type. C.   Run the new Delegation Wizard for the zone. D.   From the properties of the zone, modify the Start Of Authority (SOA) record. Answer: B Explanation: The Zone would need to be changed to a AD integrated zone When you use directory-integrated zones, you can use access control list (ACL) editing to secure a dnsZone object container in the directory tree. This feature provides detailed access to either the zone or a specified resource record in the zone. For example, an ACL for a zone resource record can be restricted so that dynamic updates are allowed only for a specified client computer or a secure group, such as a domain administrators group. This
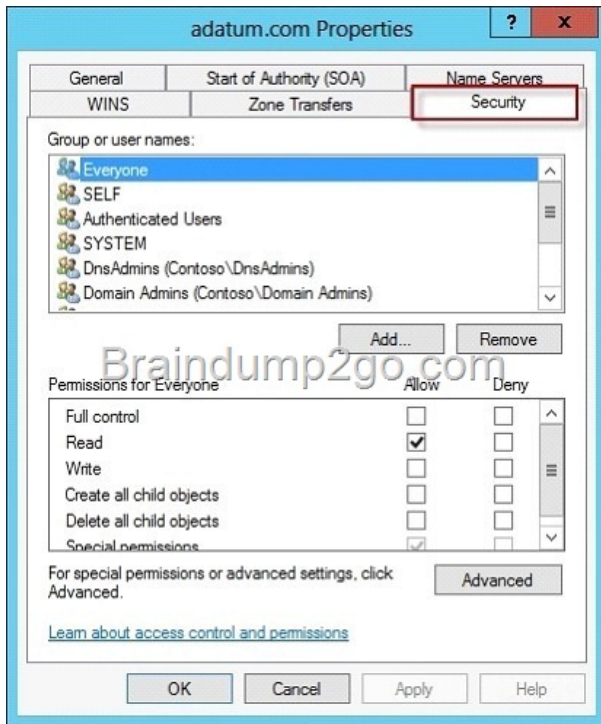
security feature is not available with standard primary zones DNS update security is available only for zones that are integrated into Active Directory. After you integrate a zone, you can use the access control list (ACL) editing features that are available in the DNS snap-in to add or to remove users or groups from the ACL for a specific zone or for a resource record. Standard (not an Active Directory integrated zone) has no Security settings:

You need to firstly change the "Standard Primary Zone" to AD Integrated Zone:

Now there's Security tab:

http://technet.microsoft.com/en-us/library/cc753014.aspx http://technet.microsoft.com/en-us/library/cc726034.aspx
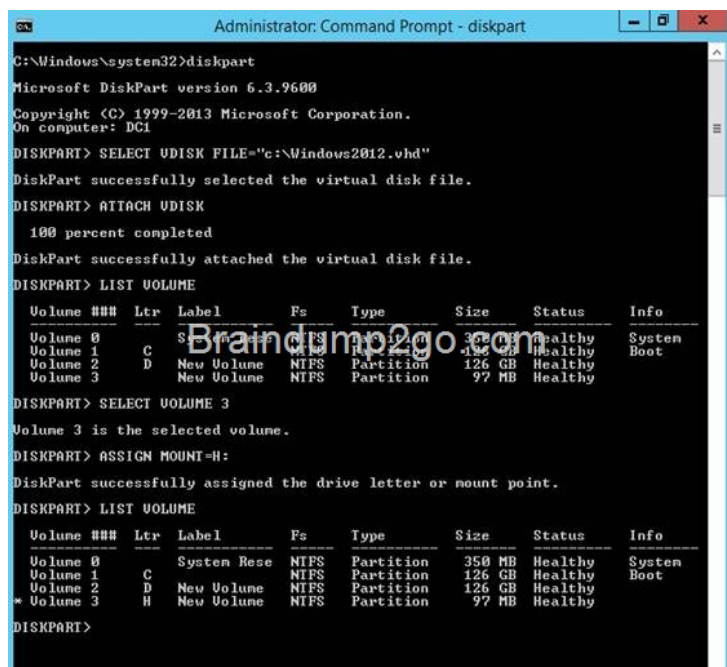http://support.microsoft.com/kb/816101 QUESTION 193 Your network contains an Active Directory domain named contoso.com.
All client computers run Windows Vista Service Pack 2 (SP2). All client computers are in an organizational unit (OU) named OU1.
All user accounts are in an OU named OU2. All users log on to their client computer by using standard user accounts. A Group
Policy object (GPO) named GPO1 is linked to OU1. A GPO named GPO2 is linked to OU2. You need to apply advanced audit
policy settings to all of the client computers. What should you do? A.   In GPO1, configure a startup script that runs auditpol.exe. B.
In GPO2, configure a logon script that runs auditpol.exe. C.   In GPO1, configure the Advanced Audit Policy Configuration
settings. D.   In GPO2, configure the Advanced Audit Policy Configuration settings. Answer: A QUESTION 194 Your network
contains two Active Directory domains named contoso.com and adatum.com. The contoso.com domain contains a server named
Server1.contoso.com. The adatum.com domain contains a server named server2.adatum.com. Server1 and Server2 run Windows
Server 2012 R2 and have the DirectAccess and VPN (RRAS) role service installed. Server1 has the default network policies and the
default connection request policies. You need to configure Server1 to perform authentication and authorization of VPN connection
requests to Server2. Only users who are members of AdatumGroup1 must be allowed to connect. Which two actions should you
perform on Server1? (Each correct answer presents part of the solution. Choose two.) A.   Network policies B.   Connection request
policies C.   Create a network policy. D.   Create a connection request policy. Answer: AD Explanation: * Connection request
policies are sets of conditions and settings that allow network administrators to designate which Remote Authentication Dial-In User
Service (RADIUS) servers perform the authentication and authorization of connection requests that the server running Network
Policy Server (NPS) receives from RADIUS clients. Connection request policies can be configured to designate which RADIUS
servers are used for RADIUS accounting. * With connection request policies, you can use NPS as a RADIUS server or as a
RADIUS proxy, based on factors such as the following: The time of day and day of the week The realm name in the connection
request The type of connection being requested The IP address of the RADIUS client QUESTION 195 You have a server that runs
Windows Server 2012 R2. You have an offline image named Windows2012.vhd that contains an installation of Windows Server
2012 R2. You plan to apply several updates to Windows2012.vhd. You need to mount Windows2012.vhd to H:. Which tool should
you use? A.   Device Manager B.   Diskpart C.   Mountvol D.   Server Manager Answer: B Explanation:

http://technet.microsoft.com/en-us/library/cc753321.aspx QUESTION 196 Your network contains an Active Directory domain named contoso.com. The domain contains a member server named Server1. Server1 runs Windows Server 2012 R2 and has the Windows Deployment Services (WDS) server role installed. You need to use WDS to deploy an image to a client computer that does not support PXE. Which type of image should you use to start the computer? A.   Install B.   Boot C.   Discover D.   Capture Answer: C QUESTION 197 Your network contains an Active Directory domain named contoso.com. All servers run Windows Server 2012 R2. The functional level of both the domain and the forest is Windows Server 2008 R2. The domain contains a domain-based Distributed File System (DFS) namespace that is configured as shown in the exhibit. (Click the Exhibit button.)

You need to enable access-based enumeration on the DFS namespace. What should you do first? A.   Install the File Server Resource Manager role service on Server3 and Server5. B.   Raise the domain functional level. C.   Delete and recreate the namespace. D.   Raise the forest functional level. Answer: C QUESTION 198 Your network contains an Active Directory domain named contoso.com. All domain controllers run Windows Server 2012 R2. The domain contains two organizational units (OUs) named OU1 and OU2 in the root of the domain. Two Group Policy objects (GPOs) named GPO1 and GPO2 are created. GPO1 is linked to OU1. GPO2 is linked to OU2. OU1 contains a client computer named Computer1. OU2 contains a user named User1. You need to ensure that the GPOs applied to Computer1 are applied to User1 when User1 logs on. What should you configure? A.   The GPO Status B.   GPO links C.   The Enforced setting D.   Security Filtering Answer: D Explanation: * GPOs cannot be linked directly to users, computers, or security groups. They can only be linked to sites, domains and organizational units. However, by using security filtering, you can narrow the scope of a GPO so that it applies only to a single group, user, or computer. * Security filtering is a way of refining which users and computers will receive and apply the settings in a Group Policy object (GPO). Using security filtering, you can specify that only certain security principals within a container where the GPO is linked apply the GPO. Security group filtering determines whether the GPO as a whole applies to groups, users, or computers; it cannot be used selectively on different settings within a GPO. Reference: Security filtering using GPMC QUESTION 199 Your company deploys a new Active Directory forest named contoso.com. The first domain controller in the forest runs Windows Server 2012 R2. The forest contains a

domain controller named DC10. On DC10, the disk that contains the SYSVOL folder fails. You replace the failed disk. You stop the Distributed File System (DFS) Replication service. You restore the SYSVOL folder. You need to perform a non-authoritative synchronization of SYSVOL on DC10. Which tool should you use before you start the DFS Replication service on DC10? A. Dfsgui.msc B.   Replmon C.   Adsiedit.msc D.   Ultrasound Answer: C Explanation: How to perform a non-authoritative synchronization of DFSR-replicated SYSVOL (like "D2" for FRS) 1. In the ADSIEDIT.MSC tool modify the following distinguished name (DN) value and attribute on each of the domain controllers that you want to make non-authoritative: CN=SYSVOL Subscription,CN=Domain System Volume,CN=DFSR-LocalSettings,CN=<the server name>,OU=Domain Controllers,DC=<domain> msDFSR-Enabled=FALSE 2. Force Active Directory replication throughout the domain. 3. Run the following command from an elevated command prompt on the same servers that you set as non-authoritative: DFSRDIAG POLLAD 4. You will see Event ID 4114 in the DFSR event log indicating SYSVOL is no longer being replicated. 5. On the same DN from Step 1, set: msDFSR-Enabled=TRUE 6. Force Active Directory replication throughout the domain. 7. Run the following command from an elevated command prompt on the same servers that you set as non-authoritative: DFSRDIAG POLLAD 8. You will see Event ID 4614 and 4604 in the DFSR event log indicating SYSVOL has been initialized. That domain controller has now done a "D2" of SYSVOL. Note: Active Directory Service Interfaces Editor (ADSI Edit) is a Lightweight Directory Access Protocol (LDAP) editor that you can use to manage objects and attributes in Active Directory. ADSI Edit (adsiedit.msc) provides a view of every object and attribute in an Active Directory forest. You can use ADSI Edit to query, view, and edit attributes that are not exposed through other Active Directory Microsoft Management Console (MMC) snap-ins: Active Directory Users and Computers, Active Directory Sites and Services, Active Directory Domains and Trusts, and Active Directory Schema. Incorrect: A: Dfsgui is for ealier versions of Windows Server. B: Replmon is for Windows 2003 and earlier. Reference: How to force an authoritative and non-authoritative synchronization for DFSR-replicated SYSVOL (like "D4/D2" for FRS) QUESTION 200 Your network contains a Hyper-V host named Server1 that hosts 20 virtual machines. You need to view the amount of memory resources and processor resources each virtual machine uses currently. Which tool should you use on Server1? A.   Windows System Resource Manager (WSRM) B.   Task Manager C.   Resource Monitor D.   Hyper-V Manager Answer: D Passing Microsoft 70-411 Exam successfully in a short time! Just using Braindump2go's Latest Microsoft 70-411 Dump: http://www.braindump2go.com/70-411.html